U.S. Department of Energy

Records Management Division

Business Continuity Plan for Electronic Records Management

February 2002

U. S. DEPARTMENT OF ENERGY

Office of the Chief Information Officer
Records Management Division

Title Page

Document Name: Business Continuity Plan

Publication Date:

Author: Records Management Division E-Mail Pilot Project Team

Approved:

Approval Date: 2/06/2002

Table of Contents

1.0 Introduction

The Office of the Chief Information Officer (CIO) ensures that the Department's recorded information is managed in an economical, effective, and efficient manner throughout its life cycle in support of mission accomplishment and accountability. This encompasses the creation, maintenance, use, disposition, donation, and preservation of records, regardless of media.

The Records Management Division has configured for its use, a record keeping system known as ForeMost Enterprise 2 with Auto Records by TrueArc, Inc. The product is being used as the CIO Records Management System (CIORMS). CIORMS will help the organization apply records management accountability to all organizational records, regardless of media. It will provide for quality electronic record keeping, and records management functionality in a desktop environment.

Disaster recovery involves strategies for recovering from a disaster. Its strategy is to minimize downtime. The strategy involves preserving data by planned back-ups and remote storage of the backed-up data. Contingency planning involves all activities that are necessary to maintain business continuity until system recovery is completed. Its strategy is to implement plans to keep business operations continuing as usual. By comparison, disaster recovery involves operational procedures for ensuring recovery of computing and networking hardware and data while business continuity involves a comprehensive plan covering people (and facilities) as well as systems and data in order to ensure that critical business processes can keep operating without interruption. This document will focus on the business continuity for CIORMS. The current focus of this pilot is toward the CIO end user community, network in general, platform, application system, and the data storage environment.

This plan will become a part of the overall Continuity of Operations Plan for the Headquarters Administrative Computer Center.

2.0 General Description

This plan outlines contingency steps to be taken in the case of a system failure, should one occur, with CIORMS in the Office of the Chief Information Officer (CIO). CIORMS automates the records management practices for hardcopy and softcopy records.

The application runs in a clustered network environment on two Compaq 8500mhz, 30 gigs of RAM servers attached to the network. A clustered network environment is one in which the two servers are connected to each other with one being in an active mode while the other remains passive, serving as the backup server. The servers connect to the SQL 7 database via ODBC (open database connectivity). The active server is the repository for the CIO file plan and records schedules that are common to the CIO. The SQL server has several smaller connecting databases, which serve as individual repositories for CIO program specific schedules and file plans. A 4gb partition created on the servers contains the NT operating system. NT Service pack 3 and Microsoft Cluster services are also installed. A 35gb RAID 5 array was created on the cluster disk drives (drive e:). This verified connectivity to the cluster disk drives from at least one node. Network connectivity is available by using Microsoft Explorer. NT Service pack 6 and Microsoft SQL version 7 are also installed on the two nodes. The SQL services were clustered.

As previously indicated, the ForeMost software is installed on both server nodes. The ForeMost services were clustered. ForeMost requires two key items; 1) Microsoft MDAC 2.5 or higher. MDAC stands for Microsoft Data Access Components. This is considered an OS upgrade and a reboot upon completion. MDAC version 2.6 seems to be a better code and also has an uninstall feature that is missing from MDAC 2.5; and 2) the latest version of the ForeMost application software.

3.0 Scope

This section will describe the operational impact of the ForeMost environment should there be an occurrence which would impact the normal processing of ForeMost due to the problems in the Headquarters Administrative Computer Center. In the event of such an occurrence, several organizations would experience the disruption.

The scope of this plan will addresses the following areas of concern:

- System Backup
- System Failure
- Contingency Steps
- Data Recovery

3.1 System Backup

The CIORMS is protected in a clustered network environment on the CIO LAN. This means, if a system failure occurs and the active server goes down, the services would then automatically activate on the passive (backup) server. When the backup server is activated, it resumes where the active server left off. The Operations Division is responsible for the servers. The CIO LAN operates in a clustered network environment to keep its computer and network systems working at a minimum level needed to achieve operational goals. When the network is backed up, CIORMS, the application and data, is automatically backed up as part of the network applications that reside on the network.

The Tivoli Storage Manager (TSM) product will be used to backup the ForeMost Server software and operating system. Backups of the clustered server will be stored in the managed tape storage system for the Enterprise (mainframe) computer.

Appropriate backup and recovery services are performed in accordance with the established Infrastructure Support Center (ISC) policy – daily, weekly, and monthly.

3.2 System Failure

If CIORMS failed in operation, the ability to electronically perform the records management storage and retrieval process would cease. Potentially, there could be loss or damage of some data contained in CIORMS. End users would be inconvenienced if the failure where to last indefinitely. If a failure were to occur, it would mean resorting to managing records manually. Productivity in managing records manually would be reduced significantly due to performing the records management process manually. The system failure would not only be inconvenient, it would be damaging. Potentially, performing the records management process could become nonexistent due to other priorities being deemed more important than records management. Damages suffered during the failure could also be costly. Consideration would have to be given to such financial factors as downtime; repair; procurement of tools to repair/replace; reinstallation; and reentry of lost data.

3.2.1 Procedures to be Carried Out In the Event of A System Failure

1. If CIORMS ceases to operate, the person discovering the system failure should analyze the situation to determine if the failure is an isolated occurrence or if other network applications are affected.

2. Call the Helpdesk Support and report the problem appropriately. If possible, provide information on the last steps performed before the system failure occurred.

3. After notify notifying the Helpdesk, inform the ForeMost System Owner of the occurrence.

4. Upon receiving an assessment of the system failure the System Owner shall notify the Program Director.

5. The Program Director shall determine if the contingency plan should be implemented and instruct the ForeMost System Owner and ForeMost System Administrator appropriately.

6. If the plan is implemented, the System Owner and Administrator will notify the CIO points of contact.

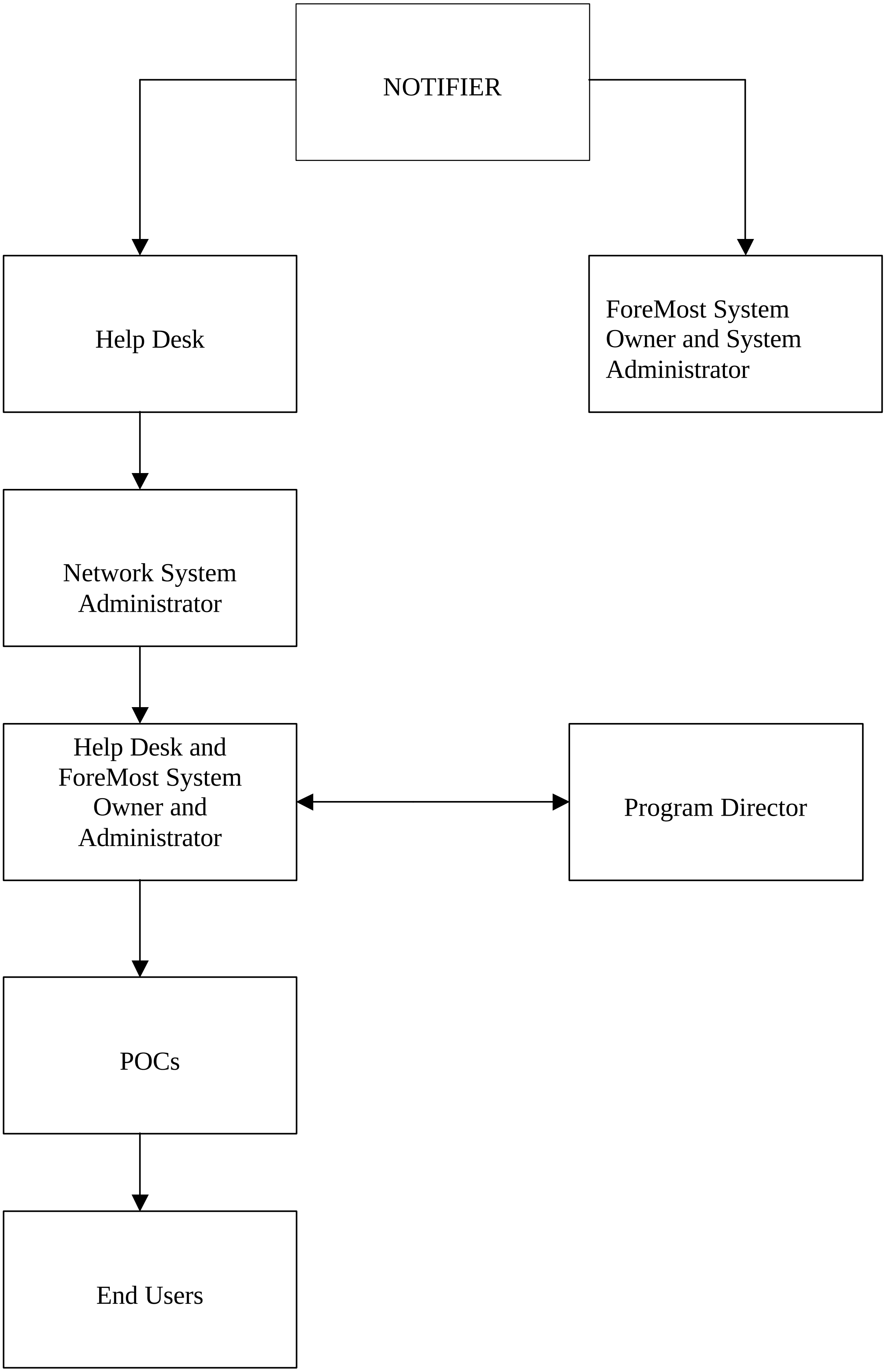
7. The CIO points of contact shall be responsible for notifying the rest of the end user community.

8. The System Owner and Administrator shall request to be kept apprised of the situation until CIORMS is back in operation.

9. Once CIORMS is back in operation, an assessment should be conducted to determine the amount of data lost, if any. A copy of the assessment should be provided to the System Owner.

10. If data is lost, the Program Director, System Owner and the ForeMost System Administrator should convene a meeting with the network System Administrator to be informed of the process that will be used for recovering/replacing the lost data.

ForeMost Notification Flow Chart


NOTIFIER
Help Desk
ForeMost System Owner and System Administrator
Network System Administrator
Help Desk and ForeMost System Owner and Administrator
Program Director
POCs
End Users

Roles and Responsibilities for Reporting a Records Management System Failure			
Role	**Name**	**Organization**	**Reporting Responsibility**
Notifier	First person who discovers problem		Is the first person to discover the system failure. Reports failure immediately to the Helpdesk.
Helpdesk Support	Denny Terpening Mary Williams	IM-40	Notifies network engineers of problem call received.
Network Engineers (LAN)	Charlie Smith Collin Batchlor	IM-40	Assesses the system failure and provides status as appropriate
ForeMost System Administrator	Gerry Clifford	IM-11	Stays in contact with the System Owner providing status of progress to resume processing
ForeMost System Owner	Lorretta Bryant	IM-11	Notifies Program Manager of system failure. Stays in contact with the System Owner and receives updates from the Helpdesk regarding recovery/restoration progress.
Program Director/Mgr	Susan L. Frey	IM-11	Has overall responsibility and accountability for the system and data. Makes decision for invoking contingency plan.
CIO Points of Contact	Yvonne Contee	IM-1	Acts as liaison between their respective CIO organizations and the Records Management Division. Notifies their respective organizations of contingency plans and keeps apprised of recovery status.
	Bernadette Crehan	IM-10	
	Bernadette Crehan	IM-11	
	Nancy Peltz	IM-12	
	Gwen Barnes	IM-20	
	Yvonne Jefferson	IM-21	
	Barbara Slagle	IM-30	
	Zelma Sheldon	IM-40	
	Yvette Howell	IM-43	
	Nancy Collins	IM-44	

3.3 Contingency Steps

If the program director deems it necessary to implement the contingency plan in order to maintain the business continuity, the following steps shall be executed:

1. Notify the appropriate points of contact that the contingency plans are being implemented. End users should be notified via their respective organizational points of contact that contingency plans are being implemented.

2. Instruct the end users to temporarily resume storing e-mail messages in an electronic file folder in Outlook. Generally, end users are already familiar with storing e-mails in electronic folders. Electronic file folders are presently used to store e-mail documents not yet categorized as records.

3. End users shall be instructed to retain all other saved documents, (word processing, spreadsheets, etc.) in their respective native applications.

4. End users shall continue the application of manual records management practices for existing hardcopy documents, i.e., filing hardcopies in appropriate file folders and applying appropriate disposal authority as when and as required.

5. Upon notification that CIORMS is back in operation, notify the end users via their organizational points of contact that CIORMS is again available and that they should immediately resume electronic record-keeping processing.

3.4 Data Recovery Steps

Data Recovery Point is the amount of acceptable information loss in the event of the system failure. The less loss that is acceptable, the more important the recovery point becomes. The loss of the records entered into CIORMS up to the point of failure is critical. If the records were not recoverable after a system failure, it would mean that a significant amount of work could be lost without assurance that it could be recreated. For example, new records filed to the ForeMost repository are not required to be stored on the creator's computer hard disk and could be lost in the event of a system failure.

Data Recovery Time is the length of interval that is acceptable between the time the system fails, and the time the system returns to operation. This is commonly known as "downtime." If delays in the ability to retrieve or the ability to file records in CIORMS went beyond a day or more, it would be damaging. The ability to file records and retrieve them must be continuously available. Capture and Retrieval of federal records must be online continuously to provide the records necessary to continue to work and to promote the use of the system. "Downtime" of the system for over long or frequent periods will discourage the end user and will eventually cause the end user to not use the system – especially if the failures occur during the initial use period. It is extremely important that CIORMS experiences a fast recovery from a system failure, as well as recovery to the exact state prior to the failure.

While Data Recovery Point and Data Recovery Time are both critical, restoration of the database is secondary to getting the system back up, online, and executing. It would be seriously damaging if CIORMS does not resume processing right where it left off. Functional performance of the CIORMS system requires that all appropriate records be captured consistently at the time of creation. Failure of the system can lead to failure of record capture at the time of creation or later. Thus, a loss of federal record in violation of NARA regulations and, more importantly, the inability to retrieve the record when needed for further work or to justify the use of government resources. Ideally, the system should be restored within 24 hours so that electronic records management processing could resume.

The responsibility for data recovery rests with the CIO network system administrator. The DOE Infrastructure Support Center (ISC) will provide assistance as necessary for problem determination and service restoration should it become necessary to recover any lost data.

4.0 Disaster Situation Personnel

ForeMost Mission-Essential Team

Position	**Name**	**Home Telephone**	**Work Telephone**
Supervisor	Susan Frey	301-540-7737	301-903-3666
Task Leader	Lorretta Bryant	301-831-1951	301-903-2164
Administrator	Gerry Clifford	301-540-8120	301-903-9608

The ForeMost Mission-Essential Management Team is responsible for performing the following:

- Evaluate the ability of *ForeMost* to **execute** assigned functions.
- Evaluate the ability of *ForeMost* to **fully accomplish** assigned functions.
- Provide a detailed briefing, to the IM-40 Disaster Recovery Coordinator, outlining the capabilities of *ForeMost*.

The Department of Energy and its support contractors must be able to identify and place individuals qualified to perform all duties described in the preceding paragraphs. Care must be taken to ensure that these individuals possess the required security clearances and have access to the keying material and cryptographic equipment required to support classified operations.

5.0 Disaster Avoidance and Prevention

The Headquarters Department of Energy (Germantown) Disaster Recovery Team provides disaster recovery services to an application such as ForeMost, which will enable it to recover from a wide range of disaster situations. Using and defining the Tivoli Storage Manager (TSM) product on the MIS (OS/390) operating system platform will easily accomplish this. It will be necessary for the DR Team to discuss the specific capabilities and requirements with the ForeMost support staff, so they will be able to develop a more accurate statement of support capabilities.